PATENT ABSTRACTS OF JAPAN

(11)Publication number : 59-036860
(43)Date of publication of application : 29.02.1984

(51)Int.Cl. G06F 15/00

(21)Application number : 57-146781
(22)Date of filing : 26.08.1982

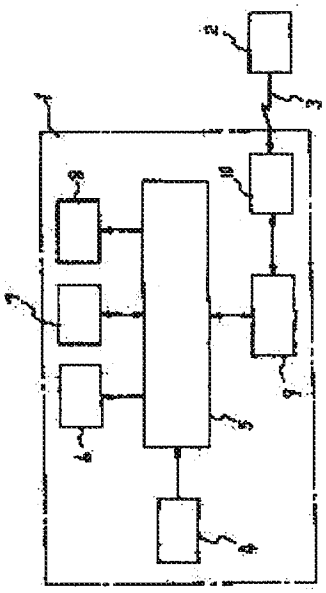
(71)Applicant : NITSUKO LTD
(72)Inventor : IWAMA TERUHIKO

(54) METHOD FOR DISCRIMINATING RELUCTANT DATA INPUT

(57)Abstract:

PURPOSE: To prevent the input of reluctant transaction due to exaction and to prevent the unjust use of a card by dividing the secret number of the card into main and sub numbers, and when the subnumber is inconsistent in spite of the coincidence of the main number, making a computer execute false data processing.

CONSTITUTION: When a sub-secret number registered as a number consisting of plural digits is inputted from an input part 4 and then a main secret number consisting of plural digits is inputted, only the sub-number is displayed 6 through a microprocessor 5 and the main number is displayed so as to be prevented from others' steal glance. Once stored 7, both secret numbers and data related to transaction are sent to a host computer HC2 in accordance with the indication of the microprocessor 5 and then only the sub-number is returned from the HC2 and displayed on a position following said display. When both the main and sub numbers coincide with eath other, the input transaction is processed. At the inconsistency of the sub-number the HC2 executes false data processing. When input is exacted from other persons, danger and unjust use of the card can be prevented by inputting a false sub-number.



⑲ 日本国特許庁 (JP)　　⑪ 特許出願公開

⑫ 公開特許公報 (A)　　昭59—36860

⑤Int. Cl.³	識別記号	庁内整理番号	⑬公開 昭和59年(1984)2月29日
G 06 F 15/00	102	6549—5B	

発明の数 1
審査請求 未請求

(全 3 頁)

⑭不本意なデータ入力の識別方式

⑦発 明 者 岩間輝彦
川崎市高津区北見方260番地日本通信工業株式会社内

⑳特 願 昭57—146781
㉒出 願 昭57(1982)8月26日

⑪出 願 人 日本通信工業株式会社
川崎市高津区北見方260番地

明 細 書

1 発明の名称

不本意なデータ入力の識別方式

2 特許請求の範囲

計算機システムとデータ入力端末装置の間で暗証番号を照合する個人識別方式において照合番号が[illegible]副暗証番号とからなり、計算機システムは照合結果により該照合番号が一致した場合のみ正規のデータ処理を行い、副暗証番号が不一致の場合は疑似のデータ処理を行わしめることを特徴とする不本意なデータ入力の識別方式。

3 発明の詳細な説明

本発明は犯罪目的でデータの入力を脅迫強要された場合に入力データを疑似的に処理することにより、被害を最少限に食止めるための不本意なデータ入力の識別方式に関する。従来の個人識別方式は使用場所が公共性のある場所で不特定多数の監視等を想定しているため、犯罪防止の方法としては使用者が入力する暗証番号[illegible]をチェックすればよかった。しかしながら将来この様の方式を使用した装置が簡易化され個人所有となり、公共性のない家庭等で使用が実現した場合、他人の脅迫強要によりA銀行からB銀行への決済時の操作がなされる犯罪に対しては本人が危険にさらされるため、余儀なく暗証番号を入力するので使用者の暗証番号のチェックだけでは犯罪防止の効果がない欠点がある。

本発明はこの欠点を除くため照合番号として個人識別の主暗証番号の他に更に本人の意志に基づく入力データで、正常な入力データか脅迫強要による入力データかを識別するための副暗証番号を設けて、該副暗証番号の正否に拘らず計算機システムは入力データを取込むようにし、犯人に察知されることなく、副暗証番号を伝達し見かけ上のデータ処理を行わしむる方式を提供する。

次に図に基づき詳細に説明する。

第1図は本発明の一実施例を示すブロックダイヤグラムである。1はデータ入力端末装置、2は計算センター等に設置された計算機システム、3は通信回線、4はデ

ータ入力部、5はデータ入力端末装置として制御処理動作を行うためのマイクロプロセッサ、6は操作手順やデータ情報を表示するための表示部、7は記憶部、8は伝送情報を出力するためのプリンター、9は該端末装置と計算機システム間でデータの送受信を行うためのデータ送受信部、10は計算機システムとデータ入力端末装置を通信回線を介して接続インターフェースである。

第1図において、データ入力部4から複数の桁からなる規定された制御証番号（例へば354とする）をテンキーまたは磁気カードで入力し続いて複数の桁からなる主暗証番号（例へば4869とする）を入力するとマイクロプロセッサ5を介して表示部6に制御証番号のみが第2図(a)のa部のように354と表示され、主暗証番号は第3者に盗視されないようにダミー記号と表示される。一方データ入力端末装置の所有者がデータ入力を他人から脅迫強要された場合、疑似データ処理する目的で前記制御証番号とは異なる任意の数、仮に538と入力すると、表示部6には第2図(b)のように538が表示され制御証番号の入力が自分の意志通りに入力されたか否かを確認することができる。

次に表示された制御証番号はマイクロプロセッサ5により記憶部7に記憶され前記データ入力部4より入力した各種データと共に記憶部7に記憶される。

次にデータ入力部4から本データ入力端末装置に該当する計算機システム2が通信回線3を介してダイヤル信号で呼び出され、計算機システム2とのデータリンクが確立すると計算機システム2よりデータ送出指示命令コードが回線インターフェース10、データ送受信部9を介してマイクロプロセッサ5で判別され、前記記憶部7に記憶されたデータの内、データ入力端末識別番号、主暗証番号、制御証番号等が計算機システム2へ送出される。計算機システム2は、前記端末識別番号、前記主暗証番号及び前記制御証番号等をメモリに一時記憶し、該制御証番号のみを前記データ入力端末装置に返送し、該端末装置の表示部6に表示された制御証番号を入力した時は第2図(c)に示すように、a部に入力した番号をb部に計算システムが確認して返送して来た番号を表示し、任意の制御証番号を入力した時は同様に第2図(b)に示すように表示し、該端末装置の所有者に該制御証番号の確認を求める。該端末装置の所有者は第2図(c)(b)に示すように、a部とb部の番号が等しい番号であればデータ入力部4に"確認"の入力をして"確認"信号をマイクロプロセッサ5、データ送受信部9及び回線インターフェース10を介して計算機システム2へ送出する。該計算機システム側は前記端末識別番号を元に主暗証番号をデコンクし命令に基づきデータの処理を行う。即ち照合番号が登録の番号と一致していれば正規のデータ処理を行い、前記データ入力端末装置1のプリンター部8に通信回線3、回線インターフェース10、データ送受信部9、マイクロプロセッサ5を介して処理応答結果をプリントアウトする。一方照合番号のうち制御証番号が一致しない場合は例へば、538の場合は疑似処理を行い結果を前記同様の方法でプリントアウトする。この場合正常処理応答の結果と疑似処理応答の結果を前記端末装置の使用者が区別することはできないようにしてあるので脅迫による疑似処理を行なった場合でも犯人にそれと気付かれることはない。尚、主暗証番号が一致しない場合は従来通り前記計算システムがデータ処理を受けないため前記端末装置の所有者は主暗証番号の入力ミスに気付く。しかし制御証番号が一致しない場合は上述のように、前記計算システムは疑似データを出力するため、所有者は入力した該制御証番号を確認する必要がある。

また、制御証番号の入力方法として、磁気カードを使用することにより通常使用の場合の入力ミスを除くとともに表示部への表示も不要となることは容易に考えられる。

以上詳細に説明したように前記データ入力端末装置の所有者は、他人から脅迫強要され照合番号を入力する時、犯罪者に見分けられずに、本人の意志に基づいたデータ処理を計算機システムに実行させることができる。一方計算機システム側においては、データ入力端末装置からの疑似データ処理命令のデータ内容が異るので、これらのデータに基づき防衛処置の行動がと

れ、被害を最少限に食止めるとともに被通報建物所有者の身の危険をかわすことができるため今後益々市場拡大するこの種のデータ処理分野に於ける効果に対して大きな効果が期待できるものである。

4. 図面の簡単な説明

第1図は本発明の一実施例を示すブロックダイヤグラム。

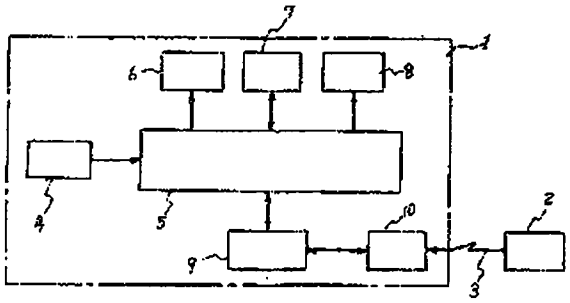
第2図(A)(B)は照合番号の表示の一実施例。(C)(D)は識別番号の入力時と計算機システムからの返送時とを比較表示した一実施例。

1. データ入力端末装置　2. 計算機システム
3. 通信回線　4. データ入力部　5. マイクロプロセッサ　6. 表示部　7. 記憶部
8. プリンター　9. データ送受信部
10. 回線インターフェース

特許出願人
日本通信工業株式会社
代表者　山田　[illegible]

(7)

第1図



第2図